Recommendations to the President's Task Force on 21st Century Policing

By Bill Schrier
Chair, Washington State Interoperability Executive Committee
State Point of Contact (SPOC), First Responder Network Authority (FirstNet)
Former Chief Technology Officer, City of Seattle, Washington

Email:	bill@schrier.org, bill.schrier@ocio.wa.gov
Twitter:	@billschrier
Blog:	http://schrier.wordpress.com
Phone:	360-902-3574

For: Ms. Laurie O. Robinson and Chief Charles H. Ramsey, Co-Chairs, and all members of President Obama's Task Force on 21st Century Policing

This testimony makes recommendations in the areas of open data, social media, technology and technology policy.

Contents

Recommendations to the President's Task Force on 21st Century Policing............................1
Social Media 2
Recommendation 1: Law Enforcement should selectively embrace Social Media 2
Recommendation 2: Use Social Media for Engagement, not just Public Information 2
Open Data 3
Recommendation 3: Be open 3
Technologies including Body Worn Video 3
Recommendation 4: Give every law enforcement officer a smart phone and tablet computer....... 3
Recommendation 5: Develop strategies which consider sensors, Next Generation 911 and the Internet of Things (IoT) 3
Recommendation 6: Implement the First Responder Network as soon as possible 4
Recommendation 7: Develop technologies to semi-automatically redact video 4
Recommendation 8: Fund not just body-worn video systems, but also costs of disclosure........... 5
Technology Policy 5
Recommendation 9: Develop and implement privacy policies which consider new technologies 5
Recommendation 10: Embrace Agile Project Management Methodology 5
Recommendation 11: Consider and engage the Street Cop.. 6
Endnotes 7

Social Media

Recommendation 1: Law Enforcement should selectively embrace Social Media

Most law enforcement agencies – sheriffs' and police departments, state police and patrol agencies, and federal entities – should actively employ multiple social media channels appropriate to their community. Such channels could be websites, Twitter, Facebook, NextDoor, Instagram, blogs, or others. But each agency will need to make a decision based upon its resources and community. A blog, such as SPDBlotter[1] employed by the Seattle Police Department, is a specific portion of a more general website used to deliver rapid updates from the scene of crimes or major incidents. A blog can quickly provide reliable, detailed information to satisfy the needs of both traditional news outlets like newspapers, radio, and television, while also meeting the needs of community newspapers, community blogs, hyperlocal blogs, Twitter feeds and Facebook posts.

Important principles include:

- Keep the channel current. Regularly refresh the content to maintain and engage the audience.
- Be responsive and quick. Post content rapidly during incidents in order to dispel rumors and maintain the audience, as was done during the Boston marathon bombing[2] and the Calgary floods of 2013[3].

Recommendation 2: Use Social Media for Engagement, not just Public Information

In the past, law enforcement has used social media primarily to "push" information to the news media and public. But, some forms of social media can also be used to "engage" the public, tweeting back-and-forth, for example, or allowing comments on blogs or Facebook pages. Such engagement can help build a "following" for the agency, help improve the public image of the agency through followers and re-posting of news, and help to rapidly dispel rumors and misinformation.

Such engagement has pitfalls. For example, the New York Police Department's ill-fated #myNYPD Twitter campaign[4] was poorly conceived. Strong policies about commenting on blogs or Facebook must be in place. Such policies would prohibit comments with profanity, political campaigning, comments disparaging others because of their race or gender, and similar restrictions.[5]

The Internet has given rise to social media, but also to a whole new set of news media sources. Many of those sources are community blogs or online news sites, which have, to some extent, replaced the community newspaper. One excellent example is the West Seattle Blog.[6] Such blogs often crowdsource information, either through comments on news articles (blog posts), via electronic mail, Twitter feeds, photo-sharing sites, or similar streams. Citizens contribute tips, comments, and photos. Generally the blog editors moderate comments and input to eliminate profane and abusive posts. Sheriffs' and police departments should share as much information as possible (recognizing legal constraints and privacy concerns) with media at the scene, on blogs, and via social media. Rapid sharing disseminates important information to the public, and energizes the public to provide information via the local blog or directly to the law enforcement agency to aid in investigation of the incident.

Open Data

Recommendation 3: Be open

Law enforcement agencies should share as much information as possible (recognizing legal constraints and privacy concerns) with the public via open data portals and similar sites. The Seattle Police Department (SPD), for example, posts detailed crime incident data, as well as, 911 call (Computer Aided Dispatch or CAD) records to data.seattle.gov. In fact, SPD posts CAD incident data for a call within a few minutes of that call taking place. The Task Force should encourage agencies to be more open in publishing such data.

Many smaller and less-well-funded law enforcement agencies do not have access to expensive open data portals such as data.gov for posting their 911 calls and crime reports. State governments should consider funding statewide open data portals to consolidate and provide a single repository for all such open data from law enforcement agencies statewide. One obstacle to such statewide portals is the lack of standardization of data outputs from various computer-aided dispatch (CAD) and records management systems (RMS). The Task Force should encourage further adoption by law enforcement agencies and software vendors of standards such as the National Information Exchange Model.[7]

Technologies including Body Worn Video

Recommendation 4: Give every law enforcement officer a smart phone and tablet computer

The first widely accepted smartphones with Internet access appeared in 2007, and the first widely accepted tablet computers in 2010. Across all sectors of the economy, businesses have adopted these tools for their employees and especially for their field forces. It is a travesty that many high school students, most package delivery drivers, and many others have these tools; but, most law enforcement professionals do not, unless the individual officer purchases the equipment personally. The applications for these devices are endless, whether it be recording witness statements (audio and visual), field report writing, criminal history searches, facial recognition and much more. Note: There are important exceptions to this lack of widespread deployment, such as San Francisco police who have embraced and deployed smart phone technology to their patrol officers, with positive results.[8]

Recommendation 5: Develop strategies which consider sensors, Next Generation 911 and the Internet of Things (IoT)

Approximately 25 billion sensors, machines and objects have been connected to the Internet[9]. Increasingly, sensors are employed in support of public safety. More than 60% of adults in the United States now have cameras, video cameras and recording devices with their smart phones. Automated license plate readers (ALPR), video surveillance cameras, body-worn and dashboard cameras are few such devices. But gunshot audio sensors, smartwatches, GPS in smart phones[10] and computers, sensors monitoring the metabolism of cops and firefighters, connected vehicles[11] (and, ultimately, automated driverless vehicles), smart grid to control electrical and water systems, and a whole variety of other sensors will be deployed in the next few years, often by private companies. These show promise to improve public safety by, for example, collecting detailed information to prosecute, prevent and ultimately eliminate driving while intoxicated. The ubiquitous deployment of sensors and video – mostly by private individuals and companies, means the ability to collect a wealth of information to quickly solve crimes as happened in the Boston Marathon bombing[12]. The Task Force should recommend further development of strategies to properly harness such technologies to improve public safety, including more rapid deployment of Next Generation 911[13] to obtain video, images and other information from the public to support law enforcement.

Recommendation 6: Implement the First Responder Network as soon as possible

The First Responder Network Authority[14] (FirstNet) is an independent authority in the federal Department of Commerce, created in 2012, funded with $7 billion from the sale of telecommunications spectrum and charged to develop a nationwide public safety wireless broadband LTE network using commercial technologies. First responders have no priority on existing commercial wireless networks built for the public, however they will have priority on FirstNet. FirstNet will be nationwide, including remote and rural areas, so that it will be able to support first responder devices wherever disasters and incidents occur. FirstNet is the most ambitious, exciting, and potentially game-changing public safety project, for the United States, in a generation.

FirstNet is the enabling network which will allow deployment and use of most of the other mobile technologies described in these recommendations, e.g. transmission of body-worn video directly to supervisors and commanders. But FirstNet faces many hurdles. It is subject to very restrictive federal personnel rules, restricting its ability to hire skilled network engineers and law enforcement professionals with incident command experience. FirstNet is also subject to the Federal Acquisition Regulation (FAR) which means network design, procurement and construction will take many years. FirstNet needs the ability to react like an entrepreneurial startup company, because technology changes rapidly. Indeed new technology and apps applicable to law enforcement appear daily. The federal government should grant FirstNet certain exceptions to these personnel rules and the FAR so it can rapidly move to design and implement this network, harnessing the latest technology, thereby supporting city, county, state and federal law enforcement officers.

Recommendation 7: Develop technologies to semi-automatically redact video

Dashboard and body-worn video cameras hold great promise for law enforcement, as President Obama recognized when he directed $75 million of funding for these systems in December, 2014.[15] But, as I've written elsewhere[16], there are many technological obstacles to realizing this vision. One of the most significant is the need to redact the faces and audio of witnesses, victims and others (for example, juveniles) before releasing video to the public. Private industry is researching and developing automated redaction, and the Seattle Police Department held a hackathon on December 19, 2014[17] to gain additional insight into the redaction challenge. As of today, such technology remains mostly in the realm of science fiction, so redaction of video prior to public disclosure is a burdensome, time-consuming, manual process[18].

Recommendation 8: Fund not just body-worn video systems, but also costs of disclosure

A major barrier to use of body-worn video is the time-consuming need to redact it before public disclosure (see recommendation 9 above). States like Florida and Washington have a very liberal public disclosure laws[19], forcing public disclosure of almost all such video Indeed, the Washing State Supreme Court has ruled[20] that all video must be released unless part of an active investigation. The public disclosure requirement is exacerbated by requests for large amounts of such video.[21] Many budget-strapped agencies, faced with funding civilian positions to redact the video rather than hiring on-the-street officers, elect not to deploy this technology.[22] Public disclosure of video is vital to improving policing. Any recommendations by the Task Force relating to body-worn and dashboard video must take into account the public disclosure laws of all states, and also recommend adequate funding to support such disclosure.

Technology Policy

Recommendation 9: Develop and implement privacy policies which consider new technologies

Ever-increasing use of social media, sensors, GPS and other location-sensing technology, the Internet of Things (IoT), widespread use of both private and public video cameras and other technologies still under development will end privacy as we've known it in the United States. These technologies will be deployed by private companies no matter how they are used by cities, counties, states and the federal government. Indeed, many private individuals willingly give up personal data by tagging faces or posting personal details on social media. Some cities, such as Seattle23, have recognized this issue and commissioned a privacy committee to address it. The task force should recommend further work to develop model policies for all levels of government to appropriately protect the privacy of everyone – the public and police officers - given the vast quantities of personal information being collected and used.

Recommendation 10: Embrace Agile Project Management Methodology

Most police information technology projects are managed using a traditional "waterfall" project management approach. "Waterfall" projects start with detailed requirements, including hundreds or thousands of technical specifications of what needs to be built. Those specifications become complex requests for proposals (RFPs) that take three-to-five years to finish. Commercial software development now uses a radically different approach – "agile". Agile methodology advocates values such as, "individuals and interactions over processes and tools", "customer collaboration over contract negotiation" and "responding to change over following a plan"[24]. In fact, such values are almost exactly how we expect officers to act on the street when confronted by incidents and strange situations. We expect them to use their training, experience, and judgment to rapidly assess and respond to each situation.

In an age of ever improving apps, smart phones, video cameras, health monitoring wearables, and connected appliances in the hands of every resident, three-to-five year technology projects often result in brand new policing tools that are already dreadfully out-of-date. Just ask any beat cop about how well the department's computer aided dispatch or field reporting software works. The Task Force should consider how "agile" can be applied to government and law enforcement's embracing of new tools, technologies and policies in public safety. Max Romanik and Christopher Webster recently published a series of articles describing how the public safety community could embrace the agile philosophy to meet these challenges.[25]

Recommendation 11: Consider and engage the Street Cop

Most road deputies, state patrol troopers, and police patrol officers are dedicated, honest professionals doing a difficult job under stressful circumstances. They make decisions in seconds which others can later review at leisure in the media, courtroom trials and years of considered analysis. With social media and technology, the voice of the street cop can be heard. Tweets-by-beat[26] is a unique Seattle police effort to automatically tweet computer-aided dispatches of officers. Tweet-along[27] allows "virtual" ride-alongs as officers tweet about their daily duties. A Seattle police officer, under the handle GoHawks206, conducted an "ask me anything" on Reddit.[28] While technically the officer violated departmental policy, the department actually embraced and encouraged it as a shift in police culture. Some public disclosure advocates actively review police video to find officers performing heroically.[29]

Often, using social media along with technology tools such as smart phones and tablet computers allows street cops to "tell their story" about their daily work. This requires supervisors, commanders, and chiefs who are willing to trust some of their officers to tweet, to blog, and to reveal how they actually work to citizens. As the Task Force considers its recommendations, it, too, should actually engage and consider the voices of these officers doing the work of protecting the public every day.

Endnotes

[1] http://spdblotter.seattle.gov/

[2] Boston Police Department and Twitter: http://www.businessweek.com/articles/2013-04-26/how-boston-police-won-the-twitter-wars-during-bomber-hunt

[3] Social media use by City of Calgary: http://www.calgaryherald.com/technology/Social+media+tools+proved+vital+2013+floods/9517574/story.html

[4] http://www.huffingtonpost.com/2014/04/22/mynypd-nypd-twitter_n_5193523.html

[5] See, for example, the City of Seattle's policy here: http://www.seattle.gov/pan/SocialMediaPolicy.htm

[6] West Seattle Blog: http://westseattleblog.com which has won numerous regional and national awards – see http://westseattleblog.com/awards/

[7] NIEM: https://www.niem.gov/aboutniem/Pages/history.aspx

[8] San Francisco use of smart phone technology: http://www.govtech.com/public-safety/Californias-JusticeMobile-Redefines-Police-Work-in-the-Field.html

[9] IoT (Internet of Things) statistics from the Federal Trade Commission: http://www.ftc.gov/news-events/blogs/business-blog/2015/01/internet-things-ftc-staff-report-new-publication-businesses

[10] GPS in smart phone – "find my iPhone" is altering law enforcement, e.g. http://seattletimes.com/html/localnews/2024979484_westneat09xml.html

[11] More about connected vehicles here: http://www.its.dot.gov/connected_vehicle/connected_vehicle_tech.htm

[12] Boston marathon bombing use of video to identify suspects: http://boston.cbslocal.com/2014/03/21/60-minutes-fbi-scanned-13000-videos-120000-photos-in-boston-marathon-bombings-probe/

[13] Next Generation 911: http://www.911.gov/911-issues/standards.html

[14] FirstNet: www.firstnet.gov

[15] President Obama funding announcement for body-worn video: http://thehill.com/homenews/administration/225583-obama-to-provide-funding-for-50000-police-body-cameras

[16] 10 Barriers to Obama's Body-worn Video Plan, *Crosscut*, December 9, 2014: http://crosscut.com/2014/12/09/technology/123137/10-barriers-obamas-police-body-cam-plan/

[17] Inside the Seattle Police Hackathon, *Geekwire*, December 20, 2014: http://www.geekwire.com/2014/seattle-police-hackathon-substantial-first-step/

[18] An example of redaction technology which might be further developed is that used by Google to blur faces in its street view: http://www.cnet.com/news/google-begins-blurring-faces-in-street-view/

[19] Washington public records act: http://apps.leg.wa.gov/rcw/default.aspx?cite=42.56

[2020] Washington State Supreme Court Ruling Fisher vs. City of Seattle: http://caselaw.findlaw.com/wa-supreme-court/1669869.html

[21] Massive Public Disclosure Requests cause Police to Hit Pause on Body Cam Programs, *Crosscut*, November 10, 2014: http://crosscut.com/2014/11/10/law-justice/122707/body-cams-washington-seattle-privacy-disclosure/

[22] Influx of records requests may force police to drop body cams, KOMO-TV, November 10, 2014: http://www.komonews.com/news/local/Police-Body-Cameras-282218401.html

[23] Seattle Privacy Committee: http://www.seattle.gov/information-technology/initiatives/privacy-initiative/privacy-advisory-committee

[24] The Agile Manifesto: http://agilemanifesto.org/

[25] Embracing agile development: https://www.emergency-management.expert/agile-development-for-public-safety-teams/

[26] Seattle Police implementation of tweets-by-beat: http://www.seattle.gov/police/tweets/

[27] Tweet-along – see example in Las Vegas here: http://www.lvmpd.com/News/PressReleases/tabid/288/EntryId/1922/LVMPD-to-Host-Tweet-Along-with-K-9.aspx

[28] Seattle Police Reddit: http://socialnewsdaily.com/16027/seattle-police-reddit-ama-against-the-rules-but-department-approves/

[29] See, for example, Tim Clemans, a civilian in Seattle who found video of a Tukwila, Washington, police officer performing CPR in the rain: http://www.liveleak.com/view?i=c40_1416141382